DEPUTY COMMISSIONER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

APR - 8 2002

MEMORANUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: for John C. Reece Dennis Szymanski
Deputy Commissioner for Modernization and
Chief Information Officer

SUBJECT: Response to Draft Report – User Activity on Most Sensitive Computer Systems Is Not Monitored (200120030)

Thank you for the opportunity to review and comment on your draft report and recommendations concerning the IRS' ability to monitor sensitive computer systems with audit trails.

In your report, you stated that the IRS still does not routinely review audit trails for its sensitive systems except for the Integrated Data Retrieval System (IDRS), the IRS' primary system for accessing taxpayer account information, and a small number of other systems. It is important to note that the IRS has been actively addressing this issue on a number of fronts. First, the IRS' system modernization is focused on ensuring that effective and efficient audit trail capabilities are included in new systems being developed. Second, the IRS is actively working its backlog of uncertified systems to ensure that they have adequate security safeguards, including audit trails. In doing this, however, the IRS has to weigh the risks and costs associated with security requirements before making an unreasonable business decision to expend an exorbitant amount of taxpayer dollars on old systems.

Our primary focus is to build the security needed in our future systems. Our current systems lack a good number of capabilities that will have to await modernization. Any enhancements to older systems have to make good business sense. We have made substantial progress in addressing IRS' audit trail shortfalls. Specifically, we have developed an audit strategy that addresses audit trails, purchased audit tools, and drafted policy guidance that significantly strengthens our posture in this area. See the attached detailed response to each of your report recommendations.

Finally, in the title for this report, we believe the placement and context for the word "sensitive" is misleading and, in fact, changes the real focus of your report. We would suggest a more appropriate title would be "User Activity on Most Systems Processing Taxpayer Data Is Not Monitored."

We appreciate your comments. If you have any questions and/or concerns, please feel free to contact me at (202) 622-6800 or Mr. Len Baptiste, Chief, Security Services at (202) 622-8910.

Attachment

User Activity on Most Sensitive Computer Systems Is Not Monitored (Audit #200120030)

RECOMMENDATION #1: A) The Office of Security should continue to work with business unit managers and the TIGTA Office of Investigations to conduct risk assessments of specific systems and locations. The assessment should be used to determine the minimum audit trail information needed to detect unauthorized accesses. **B)** The Systems Support Division should test the impact of the auditing requirements on system capacity. **C)** Depending on the test results and identification of required resources, the Office of Security, ITS, and business unit managers should coordinate to balance audit trail requirements with system capacity needs. **D)** The Systems Support Division should then identify capacity requirements and procure the hardware necessary to enable auditing.

ASSESSMENT OF CAUSE:

IRS lacks the risk assessments that are needed to determine audit trail requirements for existing and modernized systems.

CORRECTIVE ACTION TO RECOMMENDATION #1:

A) Security Services (formerly Office of Security) will continue to work with business unit managers and the TIGTA Office of Investigations to conduct risk assessments of specific systems and locations. Security Services is also partnering with ITS to conduct Risk Assessments of Tier III systems, as part of an effort to certify and accredit the Windows NT 4.0 Servers Infrastructure. Additionally, it will provide support to conduct a full risk assessment at key facilities. In addition, sites will be provided with computer-aided utilities, to enable them to tailor the risk assessments to their own areas, with assistance from Security Services.

Recognizing that capturing audit trail information is critical for all tiers and all systems, Security Policy Support and Oversight, within Security Services, is currently developing an audit strategy that includes identifying specific audit trail criteria. The first phase of this strategy is the Functional Audit Requirements document, which was recently released. The second phase is the Strategic Auditing Plan for implementing auditing control techniques for information technology systems. The final phase will be the creation of an Audit Law

Enforcement Manual (LEM). Implementation of the LEM and all audit requirements for all IRS systems will be included in this extensive third phase.

B) Security Policy Support and Oversight will work with Enterprise Operations to ensure that all system capacity testing is performed for each tier to ensure that production systems will not be adversely affected by the implementation of all audit requirements.

C) If identified results are negative upon completion of system capacity testing by Enterprise Operations, Security Policy Support and Oversight will coordinate and partner with business units and ITS to support the appropriate balance between audit requirements and system capacity and service levels.

D) If more capacity is needed and acquiring it makes business sense, Security Policy Support and Oversight will work with System Engineering and other ITS organizations to support the case for additional capacity.

IMPLEMENTATION DATE:

A) December 1, 2003
B) December 1, 2004
C) December 1, 2004
D) December 1, 2004

RESPONSIBLE OFFICIAL:

A) Director, Security Policy Support and Oversight
B) Director, Enterprise Operations
C) Director, Enterprise Operations
D) Director, Enterprise Operations

RECOMMENDATION #2: The Deputy Commissioner for Modernization & CIO should identify and address system capacity shortfalls to ensure that mainframe, Unix, and Windows NT system activity will be logged and stored.

ASSESSMENT OF CAUSE:

Inadequate system capacity for audit trails that are needed to monitor user activity on computer systems.

CORRECTIVE ACTION TO RECOMMENDATION #2:

Information Technology Services (ITS) will work with Security Services to determine the appropriate thresholds for auditable events. ITS will be responsible for establishing the capacity size of the workload associated with collecting and storing data on mainframe, UNIX, and Windows NT. ITS will also determine system resources needed, identify potential funding sources, and deploy the resources to support the auditing workload.

IMPLEMENTATION DATE:

December 1, 2004

RESPONSIBLE OFFICIAL:

Director, Enterprise Operations

RECOMMENDATION #3: The Deputy Commissioner for Modernization & CIO should ensure that ITS management obtains and uses automated audit reporting tools for the Unix and Windows NT operating systems. The availability of audit reporting tools for mainframe systems should also be explored.

ASSESSMENT OF CAUSE:

IRS lacks the audit trail tools needed to monitor user activity on computer systems.

CORRECTIVE ACTION TO RECOMMENDATION #3:

Several actions are underway to address this issue. The IRS procured a site license for Aelita Software Suite, which will allow NT audit logs to be captured and reported. Procedures are being developed to support this effort. The training of staff in use of the tools is being coordinated and will begin Spring 2002, with implementation scheduled for the Summer 2002.

For Tier II SUN E10K and E15K Consolidated systems, IRS has purchased two products from the eTrust Suite--Access Control and Audit tool. Both products are currently being analyzed to determine the appropriate configuration for implementation in the consolidated environment. A task group was established to draft the access control matrix and to recommend the proper configuration of the audit tool by applying current audit requirements.

In regard to mainframe systems, reporting tools already exist (i.e., Log Analyzer on SCRS/UNISYS, and Vanguard Reporter on IBM systems) and their expanded use will be pursued. Analytical tools to audit configurations of mainframe operating systems and applications will be explored.

IMPLEMENTATION DATE:

December 1, 2004

RESPONSIBLE OFFICIAL:

Director, Security Policy Support and Oversight

RECOMMENDATION #4: The Office of Security, in conjunction with ITS and business unit managers, should develop guidelines for use in conducting mainframe, Unix and Windows NT operating system audit trail reviews, including procedures to ensure the required reviews are conducted and documented. The TIGTA Office of Investigations should be consulted to ensure that procedures are adequate for investigative purposes.

ASSESSMENT OF CAUSE:

IRS does not have adequate guidelines for audit trail reviews of mainframe, UNIX and Windows NT operating systems.

CORRECTIVE ACTION TO RECOMMENDATION #4:

Several actions were taken or are underway to address this recommendation. Specifically, the IRS has developed functional audit requirements for all IRS systems. As part of this effort, IRS provided them to TIGTA for review and coordination. The IRS is developing guidelines for NT auditing.

Recognizing that the capture of audit trail information is a critical issue for all tiers and all systems, Security Policy Support and Oversight is currently developing an audit strategy that includes identifying specific audit trails criteria. The first phase of this strategy is the Functional Audit Requirements document, which was recently released. The second phase is the Strategic Auditing Plan for implementing auditing control techniques for information technology systems. The final phase will be creation of an Audit Law Enforcement Manual (LEM). Implementation of the LEM and all audit requirements for all IRS systems are included in an extensive third phase.

IMPLEMENTATION DATE:

December 1, 2004

RESPONSIBLE OFFICIAL:

Director, Security Policy Support and Oversight

RECOMMENDATION #5: The Office of Security should work with business unit managers to develop auditing guidelines for all sensitive system applications that do not already have them. The audit trail review requirements included in these guidelines should be based on risk.

ASSESSMENT OF CAUSE:

The IRS lacks the audit trail guidelines needed for sensitive systems applications.

CORRECTIVE ACTION TO RECOMMENDATION #5:

Recognizing that the capture of audit trail information is a critical issue for all tiers and all systems, Security Policy Support and Oversight is currently developing an audit strategy that includes identifying specific audit trails criteria. The first phase of this strategy is the Functional Audit Requirements document, which was recently released. The second phase is the Strategic Auditing Plan for implementing auditing control techniques for information technology systems. The final phase will be creation of an Audit Law Enforcement Manual (LEM). Implementation of the LEM and all audit requirements for all IRS systems are included in an extensive third phase.

The audit procedures will be developed and tested by a task group that will include representatives from the Business Units and MITS organizations. Each representative unit will be responsible for identifying critical files and directories that must be audited, using a risk-based approach. This approach will be addressed in the procedures.

IMPLEMENTATION DATE:

December 1, 2005

RESPONSIBLE OFFICIAL:

Director, Security Policy Support and Oversight

RECOMMENDATION #6: The Office of Security should coordinate with business unit managers to identify those individuals responsible for conducting audit trail reviews for all sensitive systems.

ASSESSMENT OF CAUSE:

Individuals responsible for conducting audit trail reviews for all sensitive systems had not been identified.

CORRECTIVE ACTION TO RECOMMENDATION #6:

Security Policy Support and Oversight, within Security Services (formerly the Office of Security), will coordinate with IRS business unit managers to identify IRS policy guidance that currently addresses audit trail review responsibility and the individuals responsible for conducting audit trail reviews. Specifically, IRM 25.10.1.4.13.4(1) states that "Audit trails must be reviewed periodically (at least annually) by designated personnel." Also, IRM 25.10.1.3.14(2)g. states that "Generating audit trails and security reports and distributing them to the appropriate manager;" is the responsibility of the Security Administrator. Business unit managers may delegate this responsibility, but only to non-bargaining unit employees per Title 5, United States Code, Section 7112(b)(7).

Tier specific guidelines and LEMs provide additional information consistent with these requirements. These guidelines will be augmented as discussed below. For Tier I, audit trail reviews are covered by the RACF LEM for IBM systems and will be addressed in proposed documentation for UNISYS systems and for the Security and Communications System (SACS). For Tier II, this issue will be included in the UNIX LEM and implemented via the e-Trust implementation for the consolidated environment. For Tier III, audit trail reviews will be included in the Aelita Implementation Project Plan and implemented as part of the Aelita rollout.

IMPLEMENTATION DATE:

December 1, 2003

RESPONSIBLE OFFICIAL:

Director, Security Policy Support and Oversight

RECOMMENDATION #7: The Deputy Commissioner for Modernization & CIO should emphasize the need for logging, storing, and reviewing sufficient audit trail information during the systems development and certification and accreditation processes for all new systems.

ASSESSMENT OF CAUSE:

IRS does not have adequate procedures for addressing audit trail requirements.

CORRECTIVE ACTION TO RECOMMENDATION #7:

The Modernization Security Office is working closely with the Business Systems Modernization Office to ensure that adequate audit trail capabilities are built into new systems. Recognizing that the capture of audit trail information is a critical issue for all tiers and all systems, Security Policy Support and Oversight is currently developing an audit strategy that includes identifying specific audit trails criteria. The first phase of this strategy is the Functional Audit Requirements document, which was recently released. The second phase is the Strategic Auditing Plan for implementing auditing control techniques for information technology systems. The final phase will be creation of an Audit Law Enforcement Manual (LEM). Implementation of the LEM and all audit requirements for all IRS systems are included in an extensive third phase.

The audit procedures will be developed and tested by a task group that will include representatives from the Business Units and MITS organizations. Each representative unit will be responsible for identifying critical files and directories that must be audited, using a risk-based approach. This approach will be addressed in the procedures. Modernization will also be represented in the task group as a critical source of information for audit criteria at the beginning of a system's life cycle.

IMPLEMENTATION DATE:

December 1, 2005

RESPONSIBLE OFFICIAL:

Director, Security Policy Support and Oversight
Director, Modernization Security

RECOMMENDATION #8: The Chief, ITS, in conjunction with the Director, Office of Security, should ensure that all recommendations in this report to improve system capacity, use audit reporting tools, develop audit trail review guidelines, and assign audit trail review responsibility are applied to the Tier II consolidation.

ASSESSMENT OF CAUSE:

Tier II consolidation efforts have not adequately included audit trail capabilities.

CORRECTIVE ACTION TO RECOMMENDATION #8:

Actions will be taken by Enterprise Operations to identify system resource (capacity) needs to support appropriate levels of auditing. Once this is completed, the hardware improvements necessary to support Tier II consolidation and audit trail workload will be identified and implemented in accordance with requirements where it makes business sense. Enterprise Operations will be responsibility for implementing the audit trail requirements.

IMPLEMENTATION DATE:

December 1, 2004

RESPONSIBLE OFFICIAL:

Director, Enterprise Operations